chapter 1

Introduction and Security Trends

Experience is merely the name men gave to their mistakes.

—Oscar Wilde, *The Picture of Dorian Gray*

In this chapter, you will learn how to

- Define computer security
- Discuss common threats and recent computer crimes that have been committed
- List and discuss recent trends in computer security
- Describe common avenues of attacks
- Describe approaches to computer security
- Discuss the relevant ethical issues associated with computer security

Why should we be concerned about computer and network security? All you have to do is check your newsfeed to find out about a variety of security problems that affect our nation and the world today. The danger to computers and networks may seem to pale in comparison to the threat of terrorist strikes, but in fact the average citizen is much more likely to be the target of an attack on their own personal computer, or a computer they use at their place of work, than they are to be the direct victim of a terrorist attack. This chapter will introduce you to a number of issues involved in securing your computers and networks from a variety of threats that may utilize any of a number of different attacks.

The Computer Security Problem

Fifty years ago, companies did not conduct business across the Internet. Online banking and shopping were only dreams in science fiction stories. Today, however, millions of people perform online transactions every day. Companies rely on the Internet to operate and conduct business. Vast amounts of money are transferred via networks, in the form of either bank transactions or simple credit card purchases. Wherever there are vast amounts of money, there are those who will try to take advantage of the environment to conduct fraud or theft. There are many different ways to attack computers and networks to take advantage of what has made shopping, banking, investing, and leisure pursuits a simple matter of "dragging and clicking" (or tapping) for many people. Identity theft is so common today that most everyone knows somebody who has been a victim of such a crime, if they haven't been a victim themselves. This is just one type of criminal activity that can be conducted using the Internet. There are many others, and all are on the rise.

Definition of Computer Security

Computer security is not a simple concept to define, and it has numerous complexities associated with it. If one is referring to a computer, then it can be considered secure when the computer does what it is supposed to do and *only* what it is supposed to do. But as was noted earlier, the security emphasis has shifted from the computer to the information being processed. Information security is defined by the information being protected from unauthorized access or alteration and yet is available to authorized individuals when required. When one begins considering the aspects of information, it is important to realize that information is stored, processed, and transferred between machines, and all of these different states require appropriate protection schemes. *Information assurance* is a term used to describe not just the protection of information, but a means of knowing the level of protection that has been accomplished.

Historical Security Incidents

By examining some of the computer-related crimes that have been committed over the last 30 or so years, we can better understand the threats and security issues that surround our computer systems and networks. Electronic crime can take a number of different forms, but the ones we examine here fall into one of two basic categories: crimes in which the computer was the target or incidents in which a computer was used to perpetrate the act (for example, there are many different ways to conduct bank fraud, one of which uses computers to access the records that banks process and maintain).

We start our tour of computer crimes with the 1988 Internet worm (Morris worm), one of the first real Internet crime cases. Prior to 1988, criminal activity was chiefly centered on unauthorized access to computer systems and networks owned by the telephone company and companies

Tech Tip

Historical Computer Security

Computer security is an ever-changing issue. Fifty years ago, computer security was mainly concerned with the physical devices that made up the computer. At the time, computers were the high-value items that organizations could not afford to lose. Today, computer equipment is inexpensive compared to the value of the data processed by the computer. Now the high-value item is not the machine, but the information that it stores and processes. This has fundamentally changed the focus of computer security from what it was in the early years. Today, the data stored and processed by computers is almost always more valuable than the hardware.

While *computer security* and *information security* both refer to a state where the hardware and software perform only desired actions and the information is protected from unauthorized access or alteration and is available to authorized users when required, the industry has centered on the term *cybersecurity* for the field.

that provided dial-up access for authorized users. Virus activity also existed prior to 1988, having started in the early 1980s.

Tech Tip

Intellectual Curiosity

In the early days of computer crime, much of the criminal activity centered on gaining unauthorized access to computer systems. In many early cases, the perpetrator of the crime did not intend to cause any damage to the computer but was instead on a quest of "intellectual curiosity"—trying to learn more about computers and networks. Today, the ubiquitous nature of computers and networks has eliminated the perceived need for individuals to break into computers to learn more about them. While there are still those who dabble in hacking for the intellectual challenge, it is more common today for the intellectual curiosity to be replaced by malicious intent. Whatever the reason, today it is considered unacceptable (and illegal) to gain unauthorized access to computer systems and networks.

The Morris Worm (November 1988)

Robert Morris, then a graduate student at Cornell University, released what has become known as the Internet worm (or the Morris worm). The worm infected roughly 10 percent of the machines then connected to the Internet (which amounted to approximately 6000 infected machines). The worm carried no malicious payload, the program being obviously a "work in progress," but it did wreak havoc because it continually reinfected computer systems until they could no longer run any programs.

Citibank and Vladimir Levin (June–October 1994)

Starting about June of 1994 and continuing until at least October of the same year, a number of bank transfers were made by Vladimir Levin of St. Petersburg, Russia. By the time he and his accomplices were caught, they had transferred an estimated $10 million. Eventually all but about $400,000 was recovered. Levin reportedly accomplished the break-ins by dialing in to Citibank's cash management system. This system allowed clients to initiate their own fund transfers to other banks.

Kevin Mitnick (February 1995)

Kevin Mitnick's computer activities occurred over a number of years during the 1980s and 1990s. Arrested in 1995, he eventually pled guilty to four counts of wire fraud, two counts of computer fraud, and one count of illegally intercepting a wire communication and was sentenced to 46 months in jail. In the plea agreement, Mitnick admitted to having gained unauthorized access to a number of different computer systems belonging to companies such as Motorola, Novell, Fujitsu, and Sun Microsystems. He described using a number of different "tools" and techniques, including social engineering, sniffers, and cloned cellular telephones.

Worcester Airport and "Jester" (March 1997)

In March of 1997, telephone services to the Federal Aviation Administration (FAA) control tower as well as the emergency services at the Worcester Airport and the community of Rutland, Massachusetts, were cut off for a period of six hours. This disruption occurred as a result of an attack on the phone network by a teenage computer "hacker" who went by the name "Jester."

The Melissa Virus (March 1999)

Melissa is the best known of the early macro-type viruses that attach themselves to documents for programs that have limited macro programming capability. The virus, written and released by David Smith, infected about a million computers and caused an estimated $80 million in damages.

The Love Letter Virus (May 2000)

Also known as the "ILOVEYOU" worm and the "Love Bug," the Love Letter virus was written and released by a Philippine student named

Onel de Guzman. The virus was spread via e-mail with the subject line of "ILOVEYOU." Estimates of the number of infected machines worldwide have been as high as 45 million, accompanied by a possible $10 billion in damages (it should be noted that figures like these are extremely hard to verify or calculate).

The Code Red Worm (2001)

On July 19, 2001, in a period of 14 hours, over 350,000 computers connected to the Internet were infected by the Code Red worm. The cost estimate for how much damage the worm caused (including variations of the worm released on later dates) exceeded $2.5 billion. The vulnerability, a buffer-overflow condition in Microsoft's IIS web servers, had been known for a month.

The Slammer Worm (2003)

On Saturday, January 25, 2003, the Slammer worm was released. It exploited a buffer-overflow vulnerability in computers running Microsoft SQL Server or SQL Server Desktop Engine. Like the vulnerability in Code Red, this weakness was not new and, in fact, had been discovered and a patch released in July of 2002. Within the first 24 hours of Slammer's release, the worm had infected at least 120,000 hosts and caused network outages and the disruption of airline flights, elections, and ATMs. At its peak, Slammer-infected hosts were generating a reported 1TB of worm-related traffic *every* second. The worm doubled its number of infected hosts every 8 seconds. It is estimated that it took less than 10 minutes to reach global proportions and infect 90 percent of the possible hosts it could infect.

Cyberwar? (2007)

In May of 2007, the country of Estonia was crippled by a massive denial-of-service (DoS) cyberattack against all of its infrastructure, firms (banks), and government offices. This attack was traced to IP addresses in Russia but was never clearly attributed to a government-sanctioned effort.

Operation Bot Roast (2007)

In 2007, the Federal Bureau of Investigation (FBI) announced that it had conducted Operation Bot Roast, identifying over 1 million botnet crime victims. In the process of dismantling the botnets, the FBI arrested several botnet operators across the United States. Although seemingly a big success, this effort made only a small dent in the vast volume of botnets in operation.

Conficker (2008–2009)

In late 2008 and early 2009, security experts became alarmed when it was discovered that millions of systems attached to the Internet were infected with the Downadup worm. Also known as Conficker, the worm was believed to have originated in Ukraine. Infected systems were not initially damaged beyond having their antivirus solution updates blocked. What alarmed experts was the fact that infected systems could be used in a secondary attack on other systems or networks. Each of these infected systems

Tech Tip

Speed of Virus Proliferation

The speed at which the Slammer worm spread served as a wakeup call to security professionals. It drove home the point that the Internet could be adversely impacted in a matter of minutes. This in turn caused a number of professionals to rethink how prepared they needed to be in order to respond to virus outbreaks in the future. A good first step is to apply patches to systems and software as soon as possible. This will often eliminate the vulnerabilities that the worms and viruses are designed to target.

was part of what is known as a *bot network* (or *botnet*) and could be used to cause a DoS attack on a target or be used for the forwarding of spam e-mail to millions of users.

U.S. Electric Power Grid (2009)

In April 2009, Homeland Security Secretary Janet Napolitano told reporters that the United States was aware of attempts by both Russia and China to break into the U.S. electric power grid, map it out, and plant destructive programs that could be activated at a later date. She indicated that these attacks were not new and had in fact been going on for years. One article in the *Kansas City Star*, for example, reported that in 1997 the local power company, Kansas City Power and Light, encountered perhaps 10,000 attacks for the entire year. By 2009, the company experienced 30–60 million attacks.

Fiber Cable Cut (2009)

On April 9, 2009, a widespread phone and Internet outage hit the San Jose area in California. This outage was not the result of a group of determined hackers gaining unauthorized access to the computers that operate these networks, but instead occurred as a result of several intentional cuts in the physical cables that carry the signals. The cuts resulted in a loss of all telephone, cell phone, and Internet service for thousands of users in the San Jose area. Emergency services such as 911 were also affected, which could have had severe consequences.

The Current Threat Environment

The threats of the past were smaller, targeted, and in many cases only a nuisance. As time has gone on, more organized elements of cybercrime have entered the picture along with nation-states. From 2009 and beyond, the cyberthreat landscape became considerably more dangerous, with new adversaries out to perform one of two functions: to deny you the use of your computer systems or to use your systems for financial gain, including theft of intellectual property or financial information such as personally identifiable information (PII).

Advanced Persistent Threats

Although there are numerous claims as to when **advanced persistent threats (APTs)** began and who first coined the term, the important issue is to note that APTs represent a new breed of attack pattern. Although specific definitions vary, the three words that comprise the term provide the key elements: advanced, persistent, and threat. *Advanced* refers to the use of advanced techniques, such as spear phishing, as a vector into a target. *Persistent* refers to the attacker's goal of establishing a long-term, hidden position on a system. Many APTs can go on for years without being noticed. *Threat* refers to the other objective: exploitation. If an adversary invests the resources to achieve an APT attack, they are doing it for some form of long-term advantage. APTs are not a specific type of attack, but rather the new means by which highly resourced adversaries target systems.

Tech Tip

Software Patches

One of the most effective measures security professionals can take to address attacks on their computer systems and networks is to ensure that all software is up to date in terms of vendor-released patches. Many of the outbreaks of viruses and worms would have been much less severe if everybody had applied security updates and patches when they were released. For the operating system that you use, go to your favorite web browser to find what patches exist for the operating system and what vulnerabilities or issues the patches were created to address.

Tech Tip

APTs

One of the major distinguishing characteristics of APTs is their desire to remain undetected. An APT typically follows these steps:

- *Infiltrate the network (typically phishing and then malware).*
- *Use malware to create a communication channel to external servers (command and control, or C2).*
- *Traverse the network and create multiple accounts/means of entry.*
- *Gather credentials and map assets.*
- *Gather data and exfiltrate it to C2.*
- *Cover tracks. Rinse and repeat.*

APTs are the instrument of choice for government hackers, and are used by Russia, China, Iran, and North Korea as means of stealing intellectual property and other information. Common names are applied by industry trade groups.

Tech Tip

Noteworthy APT Groups

In no particular order, here's a list of several noteworthy APT groups:

- ***Lazarus Group (North Korea)*** *Targets U.S. and South Korea. Responsible for Sony hack. Employs ransomware.*
- ***Equation Group (U.S. government)*** *Targets U.S. adversaries. Employs zero-days and EternalBlue.*
- ***APT28/Fancy Bear (Russia)*** *Targets the U.S. and the DNC. Employs spear-phishing.*
- ***Sandworm (Russian military intelligence)*** *Responsible for the Ukrainian grid attacks and the destructive NotPetya.*
- ***APT33/Elfin (Iran)*** *Targets Saudi Arabia. Responsible for Shamoon.*
- ***APT18/Dynamite Panda (China)*** *Targets U.S. Employs trojans, ransomware, and Gh0st RAT.*
- ***APT19/Codoso Group (China)*** *Targets U.S. legal and investment firms.*
- ***APT1/Comment Crew (China)*** *Targets everyone. Known as PLA Unit 61398. Employs spear-phishing.*

For more information, refer to https://www.fireeye.com/current-threats/apt-groups.html.

GhostNet (2009)

In 2009, the Dalai Lama's office contacted security experts to determine if it was being bugged. The investigation revealed it was, and the spy ring that was discovered was eventually shown to be spying on over 100 countries' sensitive missions worldwide. Researchers gave this APT-style spy network the name GhostNet, and although the effort was traced back to China, full attribution was never determined.

Operation Aurora (2009)

Operation Aurora was an APT attack first reported by Google, but it also targeted Adobe, Yahoo!, Juniper Networks, Rackspace, Symantec, and several major U.S. financial and industrial firms. Research analysis pointed to the People's Liberation Army (PLA) of China as the sponsor. The attack ran for most of 2009 and operated on a large scale, with the groups behind the attack consisting of hundreds of hackers working together against the victim firms.

Stuxnet, Duqu, and Flame (2009–2012)

Stuxnet, Duqu, and Flame represent examples of state-sponsored malware. Stuxnet was a malicious worm designed to infiltrate the Iranian uranium enrichment program, to modify the equipment and cause the systems to fail in order to achieve desired results and in some cases even destroy the equipment. Stuxnet was designed to attack a specific model of Siemens programmable logic controller (PLC), which was one of the clues pointing to its objective—the modification of the uranium centrifuges. Although neither the United States nor Israel has admitted to participating in the attack, both have been suggested to have had a role in it.

Duqu (2011) is a piece of malware that appears to be a follow-on of Stuxnet, and has many of the same targets, but rather than being destructive in nature, Duqu is designed to steal information. The malware uses command-and-control (C2) servers across the globe to collect elements such as keystrokes and system information from machines and deliver them to unknown parties.

Flame (2012) is another piece of modular malware that may be a derivative of Stuxnet. Flame is an information collection threat, collecting keystrokes, screenshots, and network traffic. It can record Skype calls and audio signals on a machine. Flame is a large piece of malware with many specific modules, including a kill switch and a means of evading antivirus detection.

Because of the open nature of Stuxnet—its source code is widely available on the Internet—it is impossible to know who is behind Duqu and Flame. In fact, although Duqu and Flame were discovered after Stuxnet, there is growing evidence that they were present before Stuxnet and collected critical intelligence needed to conduct the later attacks. The real story behind these malware items is that they demonstrate the power and capability of nation-state malware.

Sony (2011)

The hacker group LulzSec reportedly hacked Sony, stealing over 70 million user accounts. The resulting outage lasted 23 days and cost Sony in excess of $170 million. One of the biggest issues related to the attack was Sony's poor response, taking more than a week to notify people of the initial attack, and then communicating poorly with its user base during the recovery period. Also notable was that although the credit card data was encrypted on Sony's servers, the rest of the data stolen was not, making it easy pickings for the disclosure of information.

Saudi Aramco (Shamoon, 2012)

In August of 2012, over 30,000 computers were shut down in response to a malware attack (named Shamoon) at Saudi Aramco, an oil firm in Saudi Arabia. The attack hit three out of four machines in the firm, and the damage included data wiping of machines and the uploading of sensitive information to Pastebin. It took 10 days for the firm to clean up the infection and restart its business network.

Data Breaches (2013–Present)

From the end of 2013 through to the time of this writing, data breaches have dominated the security landscape. Target Corporation announced its breach in mid-December 2013, stating that the hack began as early as "Black Friday" (November 29) and continued through December 15. Data thieves captured names, addresses, and debit and credit card details, including numbers, expiration dates, and CVV codes. In the end, a total of 70 million accounts were exposed. Following the Target breach, Home Depot suffered a breach of over 50 million debit and credit card numbers in 2014.

JPMorgan Chase also had a major data breach in 2014, announcing the loss of 77 million account holders' information. Unlike Target and Home Depot, JPMorgan Chase did not lose account numbers or other crucial data

elements. JPMorgan Chase also mounted a major PR campaign touting its security program and spending in order to satisfy customers and regulators of its diligence.

At the end of 2014, Sony Pictures Entertainment announced that it had been hacked, with a massive release of internal data. At the time of this writing, hackers have claimed to have stolen as much as 100 terabytes of data, including e-mails, financial documents, intellectual property, personal data, HR information … in essence, almost everything. Additional reports indicate the destruction of data within Sony; although the extent of the damage is not known, at least one of the elements of malware associated with the attack is known for destroying the master boot record (MBR) of drives. Attribution in the Sony attack is now assigned to the North Korean APT team called the Lazarus Group.

In September of 2016, Yahoo! announced that it had been a victim of a data breach during the 2013–2014 timeframe in which 3 billion user accounts, representing over 500 million users, including real names, e-mail addresses, dates of birth, and telephone numbers, were looted by an apparent nation-state hacking group. This revelation came out during Verizon's acquisition of Yahoo! for $4.4 billion, a figure that was down nearly $400 million as a result of the breach.

Nation-State Hacking (2013–Present)

Nation-states have become a recognized issue in security—from the Great Firewall of China to modern malware attacks from a wide range of governments. Threat intelligence became more than a buzzword in 2014 as firms such as CrowdStrike exposed sophisticated hacking actors in China, Russia, and other countries. Today, numerous security firms track various APT groups as the attackers go after companies across the globe.

Not all threats are from China. Russia is credited with its own share of malware. Attribution is difficult, and sometimes the only hints are clues, such as the timelines of command-and-control servers for Energetic Bear, an attack on the energy industry in Europe from the Dragonfly Group. The Regin platform, a complete malware platform, possibly in operation for over a decade, has been shown to attack telecom operators, financial institutions, government agencies, and political bodies. Regin is interesting because of its stealth, its complexity, and its ability to hide its command-and-control network from investigators. Although highly suspected to be deployed by a nation-state, its attribution remains unsolved. Russia's military intelligence service has been connected to the hacking group Sandworm, which launched destructive attacks against the Ukrainian electric grid, and with NotPetya, a destructive malware attack that hit across Europe, the U.S., and many other countries.

In 2015, data breaches and nation-state hacking hit new highs with the loss of over 20 million sensitive personnel files from the computers at the U.S. Office of Personnel Management (OPM). This OPM loss, reportedly to China, was extremely damaging in that the data loss consisted of the complete background investigations on peoples who had submitted security clearances. These records detailed extensive personal information on the applicants and their family members, providing an adversary with detailed intelligence knowledge. In the same year it was reported that e-mail systems in the Department of State, the Department of Defense,

Tech Tip

Data Breaches

Are you on one of the following lists?

- ***Adobe, 2013*** *153 million records*
- ***Adult Friend Finder, 2016*** *400+ million records*
- ***eBay, 2014*** *145 million records*
- ***Equifax, 2017*** *147 million records*
- ***Heartland Payment Systems, 2008*** *134 million credit cards*
- ***LinkedIn, 2012/2016*** *165 million accounts*
- ***Marriott International, 2014–18*** *500 million records*
- ***My Fitness Pal, 2018*** *150 million accounts*
- ***MySpace, 2013*** *360 million accounts*
- ***NetEase, 2015*** *235 million accounts*
- ***Sina Weibo, 2020*** *538 million accounts*
- ***Yahoo!, 2013–14*** *3 billion accounts*
- ***Zynga, 2019*** *218 million accounts*

Check out https://haveibeenpwned.com/ to see if you are.

Operation Night Dragon was the name given to an intellectual property attack executed against oil, gas, and petrochemical companies in the United States. Using a set of global servers, attackers from China raided global energy companies for proprietary and highly confidential information such as bidding data for leases. The attack shed new light on what constitutes critical data and associated risks.

and the White House had been compromised, possibly by both Russia and China. The sensitive nuclear negotiations in Switzerland between the U.S., its allies, and Iran were also reported to have been subject to electronic eavesdropping by parties yet unknown.

Infrastructure Attacks

From the era of Stuxnet and extending to today, critical infrastructures have been attacked across the globe. The reasons for this are many, but the issues are consistent—critical infrastructures are controlled by computer systems, and these systems are vulnerable to attack. The list of sites is wide, but a couple worthy of mention are the Ukrainian electric grid and the Safety Instrumentation System Attack (TRITON).

Ukraine Electric Grid

On December 23, 2015, Ukraine suffered the first known successful cyber-attack against an electric grid. The result was a temporary disruption to customers of three energy distribution companies as well as damaged equipment and operations. Electricity was restored via moving to manual operation of the grid, but full restoration of grid capabilities took more than a year as equipment was damaged, forcing replacement and complete rebuilding of the architecture of the control systems. This attack was not a spur-of-the-moment attack but rather an attack that, after complete analysis, took over nine months, from the initial phishing attack to the turning off of systems. This attack has been attributed to the Russian government, primarily due to the use of the BlackEnergy3 malware from the Sandworm group. Again in 2016, the grid was attacked, again for political reasons, but using different tools and different tactics.

Safety Instrumentation System Attack (TRITON)

In 2017, security technicians discovered a new form of malware in a Saudi Arabian petrochemical plant. This malware targeted the plant's safety instrumentation systems, making this an interesting attack because, on its face, it does nothing. During normal operations, the safety instrumentation system just sits there, but in the event of something going wrong with the plant operations, the safety instrumentation system is there to protect life and property. So this attack is not meant to gather information, or to turn off lights, but rather it is a part of a bigger attack to cause even greater damage. This is less of an attack and more of a test of a larger, more menacing foe—someone who is willing to not just turn things off, but wants to break things, and potentially hurt people.

Ransomware

Ransomware is not a new threat from the theoretical perspective, as the first versions date back to the mid-to-late 1990s. However, its use was virtually nonexistent until recently. Today, ransomware ranks as one of the top threats, having grown steadily since 2012, and now representing a $1 billion a year criminal enterprise. Most current ransomware attacks use a hybrid encrypting scheme, locking the files on a victim's computer until a ransom is paid. In 2017, two major ransomware events occurred.

WannaCry

In May of 2017, WannaCry spread as an encrypting worm, hitting Microsoft Windows systems that had not been patched against a Server Message Block (SMB) vulnerability. Particularly hard hit was the British National Health Service, where more than 150 hospitals and more than 70,000 medical devices were affected over a four-day period. Estimates of the economic impact of WannaCry exceed US$4 billion due to lost time and recovery costs.

NotPetya

One of the most destructive major ransomware events was called Petya/NotPetya and occurred in June of 2017, immediately after WannaCry. Petya is a strain of ransomware that dates back to 2016 and utilizes some of the same vulnerabilities that were used by WannaCry. When a new variant of ransomware appeared on the heels of WannaCry, and used the same structures, it was considered by some to be another Petya variant. This version had several differences; most critically there was no recovery option, so Kaspersky Labs dubbed it NotPetya to specifically separate it from Petya. NotPetya was a set of malware deployed in Ukraine by Sandworm and unfortunately spread in the wild, hitting other firms.

SolarWinds Attack

In late 2020, the cybersecurity firm FireEye discovered that the SolarWinds product Orion had been compromised by an attacker. Further investigation showed that this attack began earlier in the year, probably in March of 2020, and had been passed to over 18,000 customers including many departments of the federal government. This was a carefully orchestrated supply chain attack that allowed foreign agents a backdoor to systems at these customers.

The attackers used Amazon Web Services cloud hosting to disguise their intrusions as benign network traffic, obfuscating their actions. Additionally, the hackers didn't use the malware planted in SolarWinds' Orion products to breach nearly a third of the victims. Instead they used other hacking techniques, which investigators are still unraveling. Given the time span, the depth of the attack, and the level of skill demonstrated by the attackers, this will be a significant event. The true number of actually compromised systems is still unknown, and this will become one of the biggest and most important attacks in history.

NotPetya has been crowned the most damaging malware attack. Total damages were roughly $10 billion, and included firms such as FedEx, Maersk, Merck, and others. A great analysis is available at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Tech Tip

State of Cybersecurity 2020

At the time of writing this edition, midway through 2020, it is interesting to see the current state of cybersecurity. What is the major attack vector used all the time? Phishing. What are the latest threats? Malware, and in many forms, including even Excel macros; in this case disguised as a COVID-19 report from Johns Hopkins. And why do these work? The two major issues are users being tricked into do something, and software that is not patched or kept up to date, providing the vulnerability for the malware. The years have changed, but not the problems.

Threats to Security

The incidents described in the previous sections provide a glimpse into the many different threats that administrators face as they attempt to protect their computer systems and networks. There are, of course, the normal natural disasters that organizations have faced for years. In today's highly networked world, however, new threats have developed that we did not have to worry about 50 years ago.

There are a number of ways we can break down the various threats. One way to categorize them is to separate threats that come from outside of the

organization from those that are internal. Another is to look at the various levels of sophistication of the attacks—from those by "script kiddies" to those by "elite hackers." A third is to examine the level of organization of the various threats—from unstructured threats to highly structured threats. All of these are valid approaches, and they in fact overlap each other. The following sections examine threats from the perspective of where the attack comes from.

Viruses and Worms

Although your organization may be exposed to viruses and worms as a result of employees not following certain practices or procedures, generally you will not have to worry about your employees writing or releasing viruses and worms. It is important to draw a distinction between the writers of malware and those who release malware. Debates over the ethics of writing viruses permeate the industry, but currently, simply writing them is not considered a criminal activity. A virus is like a baseball bat; the bat itself is not evil, but the inappropriate use of the bat (such as to smash a car's window) falls into the category of criminal activity. (Some may argue that this is not a very good analogy since a baseball bat has a useful purpose—to play ball—whereas viruses have no useful purpose. In general, this is true, but in some limited environments, such as in specialized computer science courses, the study and creation of viruses can be considered a useful learning experience.)

Cross Check

Malware

Viruses and worms are just two types of threats that fall under the general heading of malware. The term *malware* comes from "malicious software," which describes the overall purpose of code that falls into this category of threat. Malware is software that has a nefarious purpose, designed to cause problems to you as an individual (for example, identity theft) or your system. More information on the different types of malware is provided in Chapter 15.

By number, viruses and worms are the most common problem an organization faces because literally thousands of them have been created and released. Fortunately, antivirus software and system patching can eliminate the largest portion of this threat. Viruses and worms generally are also nondiscriminating threats; they are released on the Internet in a general fashion and aren't targeted at a specific organization. They typically are also highly visible once released, so they aren't the best tool to use in highly structured attacks where secrecy is vital.

Intruders

The act of deliberately accessing computer systems and networks without authorization is generally referred to as **hacking**, with individuals who conduct this activity being referred to as **hackers**. The term hacking also applies

to the act of exceeding one's authority in a system. This would include authorized users who attempt to gain access to files they aren't permitted to access or who attempt to obtain permissions they have not been granted. While the act of breaking into computer systems and networks has been glorified in the media and movies, the physical act does not live up to the Hollywood hype. Intruders are, if nothing else, extremely patient, since the process to gain access to a system takes persistence and dogged determination. The attacker will conduct many pre-attack activities in order to obtain the information needed to determine which attack will most likely be successful. Typically, by the time an attack is launched, the attacker will have gathered enough information to be very confident that the attack will succeed.

Generally, attacks by an individual or even a small group of attackers fall into the **unstructured threat** category. Attacks at this level generally are conducted over short periods of time (lasting at most a few months), do not involve a large number of individuals, have little financial backing, and are accomplished by insiders or outsiders who do not seek collusion with insiders. Intruders, or those who are attempting to conduct an intrusion, definitely come in many different varieties and have varying degrees of sophistication (see Figure 1.1). At the low end technically are what are generally referred to as **script kiddies**, individuals who do not have the technical expertise to develop scripts or discover new vulnerabilities in software but who have just enough understanding of computer systems to be able to download and run scripts that others have developed. These individuals generally are not interested in attacking specific targets but instead simply want to find any organization that may not have patched a newly discovered vulnerability for which they have located a script to exploit the vulnerability. It is hard to estimate how many of the individuals performing activities such as probing networks or scanning individual systems are part of this group, but it is undoubtedly the fastest growing group, and the vast majority of the "unfriendly" activity occurring on the Internet is probably carried out by these individuals.

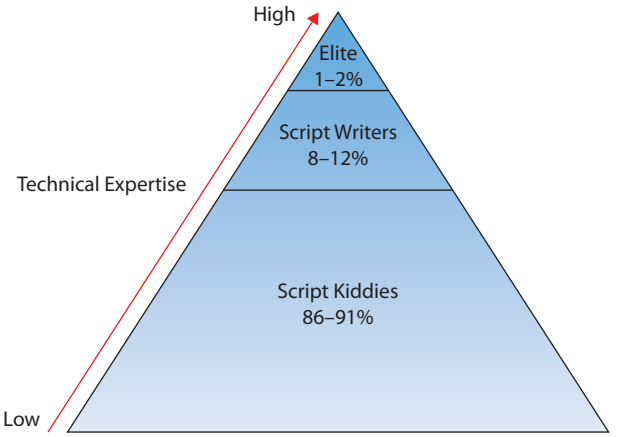


Figure 1.1 Distribution of attacker skill levels

At the next level are those people who are capable of writing scripts to exploit known vulnerabilities. These individuals are much more technically competent than script kiddies and account for an estimated 8 to 12 percent of malicious Internet activity. At the top end of this spectrum are those highly technical individuals, often referred to as **elite hackers**, who not only have the ability to write scripts that exploit vulnerabilities but also are capable of discovering new vulnerabilities. This group is the smallest of the lot, however, and is responsible for, at most, only 1 to 2 percent of intrusive activity.

Competitors as adversaries? In today's technology-dominated workplace, it should not be a surprise that competitors can be adversaries to your computer systems. Although hacking is an illegal activity, this has not prevented unscrupulous entities from attacking their competition, whether via denial of service, espionage, or fraud.

Insiders

It is generally acknowledged by security professionals that insiders are more dangerous in many respects than outside intruders. The reason for this is simple—insiders have the access and knowledge necessary to cause immediate damage to an organization. Most security is designed to protect

against outside intruders and thus lies at the boundary between the organization and the rest of the world. Insiders may actually already have all the access they need to perpetrate criminal activity such as fraud. In addition to unprecedented access, insiders also frequently have knowledge of the security systems in place and are better able to avoid detection. Attacks by insiders are often the result of employees who have become disgruntled with their organization and are looking for ways to disrupt operations. It is also possible that an "attack" by an insider may be an accident and not intended as an attack at all. An example of this might be an employee who deletes a critical file without understanding its critical nature.

As a U.S. Army soldier, Chelsea Manning began funneling classified and sensitive documents to WikiLeaks in 2010, including over a quarter of a million diplomatic cables, and was arrested and eventually convicted. This case illustrates how damaging an insider can be, as the damage done to international relations is still ongoing.

Employees are not the only insiders that organizations need to be concerned about. Often, numerous other individuals have physical access to company facilities. Custodial crews frequently have unescorted access throughout the facility, often when nobody else is around. Other individuals, such as contractors and partners, may have not only physical access to the organization's facilities but also access to computer systems and networks. A contractor involved in U.S. Intelligence computing, Edward Snowden, was charged with espionage in 2013 after he released a wide range of data illustrating the technical capabilities of U.S. Intelligence surveillance systems. He was the ultimate insider, with his name becoming synonymous with the insider threat issue.

Between Manning and Snowden, the United States government and its intelligence agencies have been challenged because of the breadth and depth of the releases. These releases damaged human agent identities, sources, methods, and virtually all types of highly restricted intelligence. And for at least a decade, if not longer, the shadow of these releases continues to mar the U.S. in international relations.

Tech Tip

The Inside Threat

One of the hardest threats that security professionals will have to address is that of the insider. Since employees already have access to the organization and its assets, additional mechanisms need to be in place to detect attacks by insiders and to lessen the ability of these attacks to succeed.

Criminal Organizations

As businesses became increasingly reliant upon computer systems and networks, and as the amount of financial transactions conducted via the Internet increased, it was inevitable that criminal organizations would eventually turn to the electronic world as a new target to exploit. Criminal activity on the Internet at its most basic is no different from criminal activity in the physical world. Fraud, extortion, theft, embezzlement, and forgery all take place in the electronic environment.

One difference between criminal groups and the "average" hacker is the level of organization that criminal elements employ in their attacks. Criminal groups typically have more money to spend on accomplishing the criminal activity and are willing to spend extra time accomplishing the task provided the level of reward at the conclusion is great enough. With the tremendous amount of money that is exchanged via the Internet on a daily basis, the level of reward for a successful attack is high enough to interest criminal elements. Attacks by criminal organizations usually fall into the **structured threat** category, which is characterized by a greater amount of

planning, a longer period of time to conduct the activity, more financial backing to accomplish it, and possibly corruption of, or collusion with, insiders.

Nation-States, Terrorists, and Information Warfare

As nations have increasingly become dependent on computer systems and networks, the possibility that these essential elements of society might be targeted by organizations or nations determined to adversely affect another nation has become a reality. Many nations today have developed to some extent the capability to conduct **information warfare**. There are several definitions for information warfare, but a simple one is that it is warfare conducted against the information and information processing equipment used by an adversary. In practice, this is a much more complicated subject, because information not only may be the target of an adversary but also may be used as a weapon. Whatever definition you use, information warfare falls into the **highly structured threat** category. This type of threat is characterized by a much longer period of preparation (years is not uncommon), tremendous financial backing, and a large and organized group of attackers. The threat may include attempts not only to subvert insiders but also to plant individuals inside of a potential target in advance of a planned attack.

An interesting aspect of information warfare is the list of possible targets available. We have grown accustomed to the idea that, during war, military forces will target opposing military forces but will generally attempt to destroy as little civilian infrastructure as possible. In information warfare, military forces are certainly still a key target, but much has been written about other targets, such as the various infrastructures that a nation relies on for its daily existence. Water, electricity, oil and gas refineries and distribution, banking and finance, telecommunications—these all fall into the category of **critical infrastructures** for a nation. Critical infrastructures are those whose loss would have severe repercussions on the nation. With countries relying so heavily on these infrastructures, it is inevitable that they will be viewed as valid targets during conflict. Given how dependent these infrastructures are on computer systems and networks, it is also inevitable that these same computer systems and networks will be targeted for a cyberattack in an information war.

As demonstrated by the Stuxnet attacks, the cyberattacks in Estonia, and the electric grid attack in Ukraine, the risk of nation-state attacks is real. There have been numerous accusations of intellectual property theft being sponsored by, and in some cases even performed by, nation-**state actors**. In a world where information dominates government, business, and economies, the collection of information is the key to success, and with large rewards, the list of characters willing to spend significant resources is high.

Tech Tip

Information Warfare

Once only the concern of governments and the military, information warfare today can involve many other individuals. With the potential to attack the various civilian-controlled critical infrastructures, security professionals in nongovernmental sectors today must also be concerned about defending their systems against attack by agents of foreign governments.

Brand-Name Attacks

By 2015, numerous firms were positioned for selling exploits, exploit kits, vulnerabilities, and other malicious items online. In an effort to develop markets and brands, groups have developed sets of malware, just as other

companies build product lines. The Sandworm Group, a group of hackers from Russia, first appeared in 2014 and then disappeared from public view until the Ukrainian electric grid attack in late 2015. All along, Sandworm had been producing and selling malware variants under the BlackEnergy name.

In some cases, the names associated with attacks, groups, or techniques come from the computer security industry, where the firms that discover them give the issue at hand a code name. This can become confusing, as multiple firms assign different names to the same issue, but over time the marketplace adjusts and settles on one name. Here are some of the recent names of interest:

- **Energetic Bear** A group of Russian hackers who used Havex malware in critical infrastructures. Also called Dragonfly.
- **Sandworm** A group of Russian hackers who have brought major issues to Ukraine via numerous attacks over the past couple of years. Also known as Electrum.
- **Shadow Brokers** A team that purportedly leaked NSA hacking tools to the public domain. They released the EternalBlue vulnerability.
- **Equation Group** A team of hackers allegedly linked to the U.S. government.
- **Regin** A team of hackers allegedly associated with the UK's GCHQ.
- **Cozy Bear and Fancy Bear** Hacker groups allegedly tied to Russia and the hacking of the Democratic National Committee (DNC) servers. Fancy Bear, also called Sofacy, is connected to Russia's GRU, and Cozy Bear, also called CozyDuke, is associated with the FSB (the Federal Security Service of the Russian Federation).
- **Vault 7** A list of leaks posted to WikiLeaks claiming to represent CIA cyber-operation methods and tools.
- **Lazarus Group** A group of hackers linked to North Korea and attacks including an $81 million bank robbery and the WannaCry ransomware attacks.
- **Comment Crew** A group of hackers associated with China. Also known as APT1.
- **Anonymous** A group of hackers that use their skills to expose perceived injustices.

Tech Tip

Confessions of a Skilled Hacker

In the summer of 2017, U.S. federal authorities arrested Marcus Hutchins, a 22-year-old UK native who had just been celebrated as the hacker who stopped the WannaCry malware. As a highly skilled hacker and self-taught reverse engineer, he seemingly used his powers for good, single-handedly finding a vulnerability in the WannaCry malware and stopping it in its tracks, worldwide. He was heralded as a hero, but his past caught up with him and he eventually pled guilty in court to writing and using malware. His whole story is worth reading, to see the good and the bad as well as the level of skill and teamwork needed to stop attacks in the current age:

https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/

Attributes of Actors

Threat actors can be divided into groups based on abilities, as shown previously in the chapter. Other ways to differentiate the threat actors are by location (internal or external), by level of sophistication, by level of resources, and by intent.

Internal/External

Internal threat actors have one significant advantage over external actors. Internal actors have access to the system, and although it may be limited to user access, it still provides the threat actor the ability to pursue their attack. External actors have an additional step: the establishment of access to the system under attack.

Level of Sophistication

As shown earlier in Figure 1.1, attacker skill or sophistication can be divided into several categories. When examining a group of threat actors, one can consider the individual skills of members of the group. There may well be a mix, with a few highly skilled individuals acting to move larger numbers of less-skilled participants. The greater the skill level, the more an individual will be expected to lead and design the attacks. When it comes to the sophistication level of the attack itself, one notable trend is that as the skill level goes up, so too does the use of minimal methods. Although zero-day attacks widely make the news, true zero-day vulnerabilities are rarely used; they are reserved for the few cases where there are no other options, because once used, they will be patched. Even with highly sophisticated and resourced nation-state teams employing APT methods, there is a surprising number of attacks being performed using old attacks, old vulnerabilities, and simple methods that take advantage of "low-hanging fruit." This is not to say that newer, more advanced methods are not used, but rather that there is an economy of mechanism in the attacks themselves, using just what is needed at each step. There is also a lot of missing data to this picture, as we do not know of the methods that have been used successfully if the threat actor remains undetected.

Resources/Funding

As mentioned earlier, criminal organizations and nation-states have larger budgets, bigger teams, and the ability to pursue campaigns for longer periods of time. Cybersecurity is challenging for attackers as well as defenders, and there are expenses associated with maintaining teams and tools used as threat actors against a system. APTs, with their penchant for long-term attacks (some lasting for years), require significant resources to engage in this type of activity, so there is a need for long-term resources that only major organizations or governments can manage over time.

Intent/Motivation

The intent or motivation behind an attack can be simple or multifold in nature. A script kiddie is just trying to make a technique work. A more skilled threat actor is usually pursuing a specific objective, such as trying to make a point as a hacktivist. At the top of the intent pyramid is the APT threat actor, whose intent or motivation is at least threefold. First is the drive to maintain persistent access mechanisms so that the threat actor has continued access. Second is the drive to remain undetected. In most APT cases that are discovered, the length of intrusion is greater than a year,

and it is many times limited by the length of logs. Third is the rationale for the attack in the first place: something of value on the network is going to be stolen. APTs do not go to all the trouble to maintain access and remain invisible just to crash a system or force a rebuild.

Security Trends

The biggest change affecting computer security that has occurred over the last 30 years has been the transformation of the computing environment from large mainframes to a highly interconnected network of smaller systems. This interconnection of systems is the Internet, and it now touches virtually all systems. What this has meant for security is a switch from a closed operating environment in which everything was fairly contained to one in which access to a computer can occur from almost anywhere on the planet. This has, for obvious reasons, greatly complicated the job of the security professional.

The type of individual who attacks a computer system or network has also evolved over the last 30 years. As illustrated by the attacks listed previously, the attackers have become more focused on gain over notoriety. Today, computer attacks are used to steal and commit fraud and other crimes in the pursuit of monetary enrichment. Computer crimes are currently big business, not just because it is hard to catch the perpetrators, but because the number of targets is large and the rewards greater than robbing local stores.

Over the past several years, a wide range of computer industry firms have begun issuing annual security reports. Among these firms is Verizon, which has issued its annual Data Breach Investigations Report (DBIR) since 2008. This report has been lauded for its breadth and depth. The 10th edition of the DBIR was published in 2017, and it analyzed more than 42,000 incidents and 1900 confirmed breaches spanning 84 countries and 20 industries. Perhaps the most valuable aspect of the DBIR is its identification of common details that result in a data breach. By the 2020 report, the size had continued to grow to a record total of 157,525 incidents, which after analysis, 3950 were confirmed to be data breaches. The cybersecurity world is not safer.

Targets and Attacks

A particular computer system is generally attacked for one of two reasons: either it is specifically targeted by the attacker or it is an opportunistic target.

Specific Target

In this case, the attacker has chosen the target not because of the hardware or software the organization is running but for another reason—perhaps a political reason. An example of this type of attack would be an individual in one country attacking a government system in another. Alternatively, the

Tech Tip

Verizon Data Breach Investigations Report

If a cybersecurity practitioner, an executive, or anyone for that matter, wanted to get a report of the trends that are occurring in today's cybersecurity arena, the Verizon Data Breach Investigations Report is the place to start. While not filled with tons of specific attack details, this document does paint the picture of what is happening to IT systems across tens of thousands of attacks and thousands of breaches—all with an eye to providing top-level guidance on what happened and why. See https://enterprise.verizon.com/resources/reports/dbir for current report.

In the early days of computers, security was considered to be a binary condition in which your system was either secure or not secure. Efforts were made to achieve a state of security, meaning that the system was secure. Today, the focus has changed. In light of the revelation that a pure state of security is not achievable in the binary sense, the focus has shifted to one of risk management. Today, the question is how much risk your system is exposed to, and from what sources.

attacker may be targeting the organization as part of a **hacktivist** attack. For example, an attacker may deface the website of a company that sells fur coats because the attacker feels that using animals in this way is unethical. Perpetrating some sort of electronic fraud is another reason a specific system might be targeted. Whatever the reason, an attack of this nature is decided upon before the attacker knows what hardware and software the organization has.

The motive behind most computer attacks falls into one of two categories:

1. To deprive someone the use of their system
2. To use someone else's system to enrich oneself

In some cases, the use of a denial-of-service attack (item 1) precedes the actual heist (item 2).

Opportunistic Target

The second type of attack, an attack against a target of opportunity, is conducted against a site that has software that is vulnerable to a specific exploit. The attackers, in this case, are not targeting the organization; instead, they have learned of a vulnerability and are simply looking for an organization with this vulnerability that they can exploit. This is not to say, however, that an attacker might not be targeting a given sector and looking for a target of opportunity in that sector. For example, an attacker may desire to obtain credit card or other personal information and might search for any exploitable company with credit card information in order to carry out the attack.

Targeted attacks are more difficult and take more time than attacks on a target of opportunity. The latter simply relies on the fact that with any piece of widely distributed software, there will almost always be somebody who either has not patched the system or has not patched it properly.

Minimizing Possible Avenues of Attack

Understanding the steps an attacker will take enables you to limit the exposure of your system and minimize those avenues an attacker might possibly exploit. There are multiple elements to a solid computer defense, but two of the key elements—patching and hardening—involve limiting an attacker's avenues of attack.

The first step an administrator can take to reduce possible attacks is to ensure that all patches for the operating system and applications are installed. Many security problems that we read about, such as viruses and worms, exploit known vulnerabilities for which patches exist. The reason such malware caused so much damage in the past was that administrators did not take the appropriate actions to protect their systems.

The second step an administrator can take is hardening the system, which involves limiting the services that are running on the system. Using only those services that are absolutely needed does two things: it limits the possible avenues of attack (those services with vulnerabilities that can be exploited) and it reduces the number of services the administrator has to worry about patching in the first place. This is one of the important early steps any administrator should take to secure a computer system. System hardening is covered in detail in Chapter 14.

Although there are no iron-clad defenses against attack, or guarantees that an attack won't be successful, you can take steps to reduce the risk of loss. This is the basis for the change in strategy from a defense-based one to one based on risk management. Risk management is covered in detail in Chapter 20.

Approaches to Computer Security

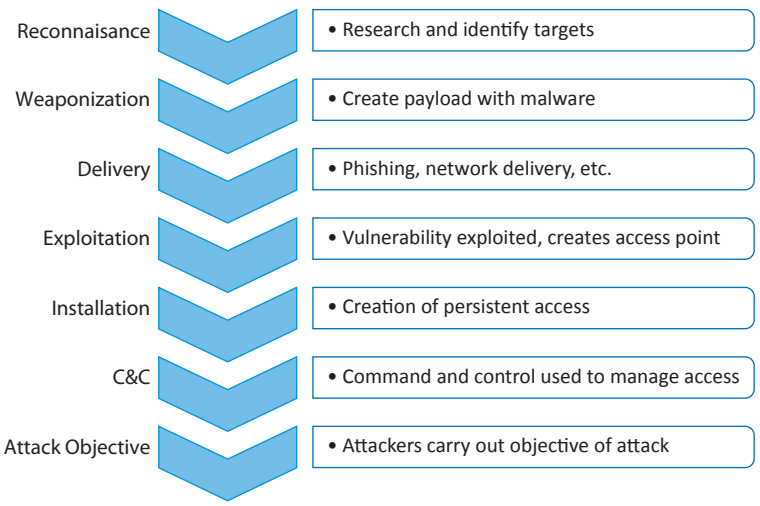
Although much of the discussion of computer security focuses on how systems are attacked, it is equally important to consider the structure of defenses. You have three major considerations when securing a system:

- **Correctness** Ensuring that a system is fully up to date, with all patches installed and proper security controls in place. This goes a long way toward minimizing risk. Correctness begins with a secure development lifecycle (covered in Chapter 19), continues through patching and hardening (Chapters 14 and 21), and culminates in operations (Chapters 3, 4, 20, and 21).
- **Isolation** Protecting a system from unauthorized use, by means of access control and physical security. Isolation begins with infrastructure (covered in Chapters 9 and 10), continues with access control (Chapters 8, 11, and 12), and includes the use of cryptography (Chapters 5, 6, and 7).
- **Obfuscation** Making it difficult for an adversary to know when they have succeeded. Whether accomplished by obscurity, randomization, or obfuscation, increasing the workload of an attacker makes it more difficult for them to succeed in their attack. Obfuscation occurs throughout all topics because it is a built-in element, whether in the form of random numbers in crypto or address space randomizations, stack guards, or pointer encryption at the operating system level.

Each of these approaches has its inherent flaws, but taken together, they can provide a strong means of system defense.

Cybersecurity Kill Chain

One of the newer methods of modeling attacks is via a **cybersecurity kill chain** (see Figure 1.2), a step-by-step process that attacks follow to target and achieve results on victim systems. Originally developed by Lockheed Martin, this framework concept provides a means for the identification and prevention of cyberintrusion activity. The framework identifies the typical steps an adversary must complete in order to achieve their objective. The kill chain concept is important because in many cases the detection of an adversary on your network will be earlier in the kill chain process, giving a firm an opportunity to break the attack pattern before actual damage is done. Modeled after kill chains used to break the lifecycle of other attackers, such as insects, the cybersecurity kill chain gives defenders a means of stopping sophisticated attackers before the damage is done by targeting the attacker's process rather than the victim machine's reaction to the delivery of terminal attack objectives. This enables teams of hunters to go track down attackers and act



• **Figure 1.2** The cybersecurity kill chain

proactively rather than defending in a reactive mode after an attack has been successful.

Threat Intelligence

Cybersecurity is a game of resource management. No firm has the resources to protect everything against all threats, and even attempting to do so would add complexity that would open up other threat avenues. One of the important decisions is where to apply one's resources in the complex landscape of cyber defense. **Threat intelligence** is a set of actions taken to properly utilize resources to target the actual threats an enterprise is facing. Threat intelligence is the actionable information about malicious actors and their tools, infrastructure, and methods. Threat intelligence includes evidence-based information as to context, mechanisms, indicators, and implications associated with a hazard to a system. It is action-oriented so it can be used to drive responses to the hazard. This is important to security teams because it steers their resources to detect threats in their network and prioritize the response to real threats. Threat intelligence is the basis of understanding adversary **tactics, techniques, and procedures (TTPs)**.

Threat intelligence is broken down into three types, with different audiences and objectives for each:

- **Strategic** Broader trends typically meant for a nontechnical audience
- **Tactical** Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience
- **Operational** Technical details about specific attacks and campaigns

Threat intelligence has become a buzzword in the security industry, with numerous firms providing services in this area. Several main forms of threat intelligence are in use today. The biggest and most comprehensive are the **Information Sharing and Analysis Centers (ISACs)** and **Information Sharing and Analysis Organizations (ISAOs)** that have been created to share information across firms. These are typically large-budget operations, with the costs and results shared among members. A second form of threat intelligence is referred to as *open source intelligence*.

In a modern enterprise, threat intelligence is a critical security operation. The information that it gathers can shape policies, operations, vulnerability management, incident response, and risk analysis efforts.

Tech Tip

Tactics, Techniques, and Procedures (TTPs)

The acronym TTP is used to describe how threat agents organize and orchestrate their efforts. Like any other organization, hackers evolve to use repeatable methods that are effective. These methods can be cataloged and understood as attack patterns, enabling defenses to have countering plays developed in advance. TTPs, or the patterns used by adversaries, are a key element of a threat intelligence program.

Open Source Intelligence

Open source intelligence (OSINT), sometimes called open source threat intelligence, is the term used to describe the processes used in the collection of threat intelligence information from public sources. There is a wide range of public sources of information concerning current cybersecurity activity. From news articles, to blogs, to government reports, there seems to be a never-ending stream of news concerning what is happening, to whom, and how. This leads to the overall topic of information sharing and the greater topic of threat intelligence (not open source).

Ethics

Any meaningful discussion about operational aspects of information security must include the topic of ethics. *Ethics* is commonly defined as a set of moral principles that guides an individual's or group's behavior. Because information security efforts frequently involve trusting people to keep secrets that could cause harm to the organization if revealed, trust is a foundational element on the people side of security. Also, trust is built on a code of ethics—a norm that allows everyone to understand expectations and responsibilities. Several different ethical frameworks can be applied to making a decision, and these are covered in detail in Chapter 24.

Ethics is a difficult topic; separating right from wrong is easy in many cases, but in other cases it is more difficult. For example, writing a virus that damages a system is clearly bad behavior, but is writing a worm that goes out and patches systems, without the users' permission, right or wrong? Do the ends justify the means? Such questions are the basis of ethical discussions that define the challenges faced by security personnel on a regular basis.

Additional References

http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

https://enterprise.verizon.com/resources/reports/dbir/

Chapter 1 Review

Chapter Summary

After reading this chapter and completing the quizzes, you should understand the following regarding security threats and trends.

Define computer security

- Computer security is defined by a system operating in a manner in which it does what it is supposed to do and only what it is supposed to do.
- Information security is defined by the information being protected from unauthorized access or alteration and yet is available to authorized individuals when required.

Discuss common threats and recent computer crimes that have been committed

- The various threats to security include viruses and worms, intruders, insiders, criminal organizations, terrorists, and information warfare conducted by foreign countries.
- A particular computer system is generally attacked for one of two reasons: it is specifically targeted by the attacker or it is a target of opportunity.
- Targeted attacks are more difficult and take more time than attacks on a target of opportunity.
- The different types of electronic crime fall into two main categories: crimes in which the computer was the target of the attack, and incidents in which the computer was a means of perpetrating a criminal act.
- One significant trend observed over the last several years has been the increase in the number of computer attacks and their effectiveness.

List and discuss recent trends in computer security

- Malicious actors use many different ways to attack computers and networks to take advantage of online shopping, banking, investing, and leisure pursuits, which have become a simple matter of "dragging and clicking" for many people.
- The biggest change that has occurred in security over the last 30 years has been the transformation of the computing environment from large mainframes to a highly interconnected network of much smaller systems.

Describe common avenues of attacks

- An attacker can use a common technique against a wide range of targets in an opportunistic attack, only succeeding where the attack is viable.
- An attacker can employ a variety of techniques against a specific target when it is desired to obtain access to a specific system.

Describe approaches to computer security

- An enterprise can use three main approaches to computer security: one based on correctness, one involving isolation, and one involving obfuscation. The ideal method is to employ all three together.

Discuss the relevant ethical issues associated with computer security

- Ethics is commonly defined as a set of moral principles that guides an individual's or group's behaviors.
- Because information security efforts frequently involve trusting people to keep secrets that could cause harm to the organization if revealed, trust is a foundational element on the people side of security.

Key Terms

advanced persistent threat (APT) *(4)*
computer security *(1)*
critical infrastructure *(13)*
cybersecurity kill chain *(18)*
elite hacker *(11)*
hacker *(10)*
hacking *(10)*
hacktivist *(17)*
highly structured threat *(13)*
Information Sharing and Analysis Center (ISAC) *(19)*
Information Sharing and Analysis Organization (ISAO) *(19)*
information warfare *(13)*
open source intelligence (OSINT) *(19)*
script kiddie *(11)*
state actors *(13)*
structured threat *(12)*
tactics, techniques, and procedures (TTPs) *(19)*
threat intelligence *(19)*
unstructured threat *(11)*

Key Terms Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. A(n) _____ is characterized by a greater amount of planning, a longer period of time to conduct the activity, more financial backing to accomplish it, and the possible corruption of, or collusion with, insiders.
2. The patterns of activities or methods associated with a specific threat actor or group of threat actors is known as a(n) _____.
3. A(n) _____ is one whose loss would have a severe detrimental impact on the nation.
4. _____ is conducted against the information and information-processing equipment used by an adversary.
5. Actors who deliberately access computer systems and networks without authorization are called _____ .
6. A(n) _____ is generally short term in nature, does not involve a large group of individuals, does not have significant financial backing, and does not include collusion with insiders.
7. A(n) _____ is a highly technically competent individual who conducts intrusive activity on the Internet and is capable of not only exploiting known vulnerabilities but also finding new vulnerabilities.
8. Actionable information about malicious actors as well as their tools, infrastructure, and methods is called _____.
9. A(n) _____ is an individual who does not have the technical expertise to develop scripts or discover new vulnerabilities in software but who has just enough understanding of computer systems to be able to download and run scripts that others have developed.
10. A(n) _____ is characterized by a much longer period of preparation (years is not uncommon), tremendous financial backing, and a large and organized group of attackers.

Multiple-Choice Quiz

1. Which threats are characterized by possibly long periods of preparation (years is not uncommon), tremendous financial backing, a large and organized group of attackers, and attempts to subvert insiders or to plant individuals inside a potential target in advance of a planned attack?
   - **A.** Unstructured threats
   - **B.** Structured threats
   - **C.** Highly structured threats
   - **D.** Nation-state information warfare threats
2. In which of the following attacks is an attacker looking for any organization vulnerable to a specific exploit rather than attempting to gain access to a specific organization?
   - **A.** Target of opportunity attack
   - **B.** Targeted attack
   - **C.** Vulnerability scan attack
   - **D.** Information warfare attack
3. The rise of which of the following has greatly increased the number of individuals who probe organizations looking for vulnerabilities to exploit?
   - **A.** Virus writers
   - **B.** Script kiddies
   - **C.** Hackers
   - **D.** Elite hackers
4. For what reason(s) do some security professionals consider insiders more dangerous than outside intruders?
   - **A.** Employees (insiders) are easily corrupted by criminal and other organizations.
   - **B.** Insiders have the access and knowledge necessary to cause immediate damage to the organization.
   - **C.** Insiders have knowledge of the security systems in place and are better able to avoid detection.
   - **D.** Both B and C.
5. Using knowledge associated with an attacker's process to find a weakness in the attack mechanism and then to catch and block the attacker is called what?
   - **A.** Open source intelligence
   - **B.** Cybersecurity kill chain
   - **C.** Active incident response
   - **D.** Defense in depth
6. What is the most common problem/threat an organization faces?
   - **A.** Viruses/worms
   - **B.** Script kiddies
   - **C.** Hackers
   - **D.** Hacktivists

7. Warfare conducted against the information and information-processing equipment used by an adversary is known as what?
   - **A.** Hacking
   - **B.** Cyberterrorism
   - **C.** Information warfare
   - **D.** Network warfare
8. An attacker who feels that using animals to make fur coats is unethical and thus defaces the website of a company that sells fur coats is an example of what?
   - **A.** Information warfare
   - **B.** Hacktivism
   - **C.** Cyber crusading
   - **D.** Elite hacking
9. Criminal organizations would normally be classified as what type of threat?
   - **A.** Unstructured
   - **B.** Unstructured but hostile
   - **C.** Structured
   - **D.** Highly structured
10. Which of the following individuals has the ability to not only write scripts that exploit vulnerabilities but also discover new vulnerabilities?
    - **A.** Elite hacker
    - **B.** Script kiddie
    - **C.** Hacktivist
    - **D.** Insider

Essay Quiz

1. Reread the various examples of computer crimes at the beginning of this chapter. Categorize each as either a crime where the computer was the target of the criminal activity or a crime in which the computer was a tool in accomplishing the criminal activity.
2. A friend of yours has just been hired by an organization as its computer security officer. Your friend is a bit nervous about this new job and has come to you, knowing that you are taking a computer security class, to ask your advice on measures that can be taken that might help prevent an intrusion. What three things can you suggest that are simple but can tremendously help limit the possibility of an attack?
3. Discuss the major difference between a target of opportunity attack and a targeted attack. Which do you believe is the more common one?

Lab Projects

• Lab Project 1.1

A number of different examples of computer crimes were discussed in this chapter. Similar activities seem to happen daily. Do a search on the Internet to see what other examples you can find. Try and obtain the most recent examples possible.

• Lab Project 1.2

Your boss just sent you a copy of the Verizon DBIR, with a note reading, "What does this mean to us?" How would you summarize the DBIR in a presentation with fewer than 10 slides in less than 10 minutes?